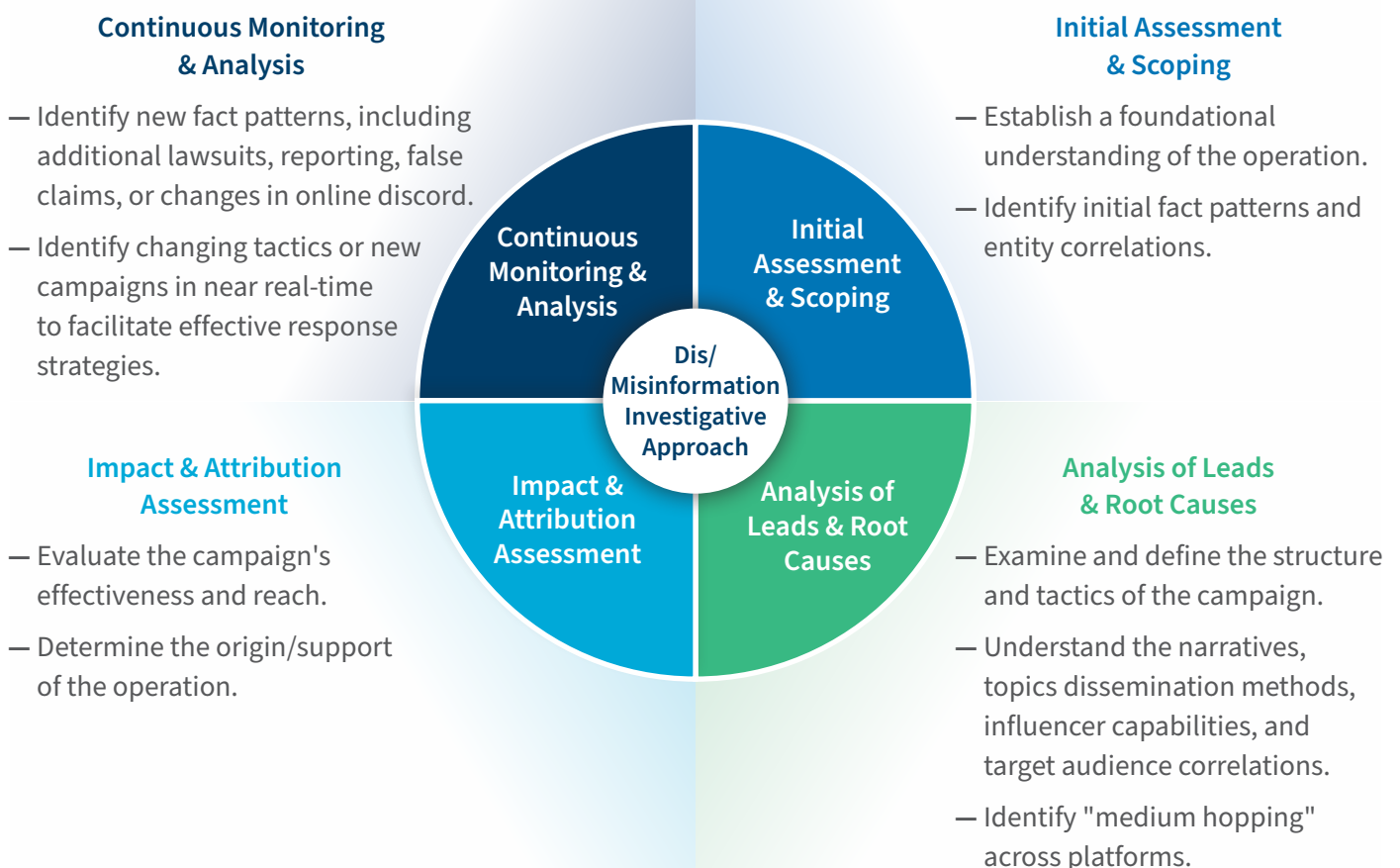# Disinformation & Misinformation Campaigns

Individuals, organizations, and government entities can find themselves the target of disinformation or misinformation campaigns aimed at destroying their brand, reputation, and enterprise value. FTI Cybersecurity provides the necessary expertise to identify and unravel these campaigns, producing conclusive findings and strategies to combat and counteract the spread of dis/misinformation.

— HOW FTI CYBERSECURITY CAN HELP

Continuous Monitoring & Analysis

— Identify new fact patterns, including additional lawsuits, reporting, false claims, or changes in online discord.

— Identify changing tactics or new campaigns in near real-time to facilitate effective response strategies.

Initial Assessment & Scoping

— Establish a foundational understanding of the operation.

— Identify initial fact patterns and entity correlations.

Impact & Attribution Assessment

— Evaluate the campaign's effectiveness and reach.

— Determine the origin/support of the operation.

Analysis of Leads & Root Causes

— Examine and define the structure and tactics of the campaign.

— Understand the narratives, topics dissemination methods, influencer capabilities, and target audience correlations.

— Identify "medium hopping" across platforms.

Dis/Misinformation Investigative Approach
- Continuous Monitoring & Analysis
- Initial Assessment & Scoping
- Analysis of Leads & Root Causes
- Impact & Attribution Assessment

Comprehensive Investigation of Dis/Misinformation Campaigns

FTI Cybersecurity experts have extensive experience leveraging the artifacts left behind by even the most skilled threat actors to recreate the phases of a dis/misinformation campaign, whether ongoing or years after the fact. Our tailored and structured approach identifies root causes and pinpoints changing tactics and targets to support strategic response efforts and determine the extent of negative impact.

Forensically Sound Methodology

OPEN-SOURCE INTELLIGENCE

— Online and social media account analysis & attribution (including the identification of real individuals vs. bot accounts)
— Username, domain, and address analysis
— Image and video analysis
— Review of public filings
— Review of financial reporting
— Review of principles, boards, and other entity relationships
— Physical surveillance when needed
— Deep and dark web monitoring

DATA & INISIGHTS

— Data science and scripting
— Metrics and narrative spread analysis
— Pattern analysis for content creation, amplification, and narrative dissemination
— Sentiment analysis
— Network structure identification
— Data visualizations

FORENSIC ANALYSIS

— Trace technical indicators to attribute sources and artifacts
— Forensic analysis on network infrastructure, mobile devices, laptops and workstations, cloud environments, and IoT devices
— Leverage real-time threat intelligence to align tactics with known threat actors, including nation-states

FTI Cybersecurity uses industry recognized and lawful best practices to carry out investigations, ensuring evidence can be preserved and referenced in litigation when needed. We leverage proven frameworks, such as the Disinformation Kill Chain, to structure our approach, and employ policies and procedures to effectively document and preserve all artifacts. We work under the direction of counsel to preserve privilege or directly on behalf of clients.

Impact Assessments

FTI Cybersecurity's investigative teams, supported by our damages experts, can document the negative financial and reputational impact caused by a dis/misinformation campaign, ultimately a necessary component of any counter litigation.

Continuous Monitoring

Dis/misinformation campaigns are less effective when identified immediately, allowing quick counter-actions. FTI Cybersecurity provides resources to monitor sources including social media, court filings, and other forums to quickly identify new tactics, phases, and targets, preparing clients for an immediate response to mitigate ongoing risk.

Mitigation

Our experts provide strategic counsel to clients in sensitive situations with legal, financial, regulatory, and reputational implications. We deploy a custom application of the fundamental incident preparedness and response components to meet client's needs.

To be crisis-ready and responsive, everyone must know their roles and responsibilities in advance. With an emphasis on training and learning, FTI Cybersecurity's preparedness planning services focus on developing best practice crisis management skills and knowledge. In addition, risk mapping and education can help clients understand their digital presence and evaluate communications methods to assess their susceptibility to coordinated dis/misinformation efforts.

Once an incident is identified, we combine the resources and tools necessary to determine the scope, impact, and appropriate response. These efforts determine the source of the incident and preserve necessary forensic artifacts. Then, our team moves into the containment, eradication, and recovery phase. Through a post-incident assessment, we detail the cost, cause, and response for the incident, along with steps that should be taken to prevent future incidents.

Bolstered by our investigative work, FTI Cybersecurity also offers clients advisory support on litigation and compliance matters as further steps to blunt the impact of dis/misinformation efforts. We help clients protect their enterprise value through evidence collection, handling, and preservation; forensic analysis; and expert witness testimony.

CASE STUDY

DISINFORMATION CAMPAIGN INVESTIGATION FOR A HIGH-PROFILE INDIVIDUAL

FTI Cybersecurity was engaged, through outside counsel, by a high-profile individual who was concerned that they were undergoing a targeted online disinformation campaign following the release of the client's product. Online sentiment appeared to have shifted negatively, and the client was seeking investigation into whether there was any coordination behind the activity.

OUR IMPACT

Our effort resulted in a conclusive final report, which included specific online accounts and posts that were at the center of the disinformation campaign and trend analysis that demonstrated the genesis and overall arch of the campaign.

A critical result of FTI Cybersecurity's investigation included multiple online personas acknowledging that they were paid to post the negative content that was then amplified to go viral.

OUR ROLE

Our investigation teams focused on a sentiment analysis to identify un-natural inflection points in online discord about the topic and the client; open-source intelligence gathering to identify specific individual accounts, across multiple online platforms, and posts that originated the shift in sentiment; and forensic analysis to preserve content across multiple user devices for ties to the disinformation campaign.

CASE STUDY

ONLINE REVIEW INVESTIGATION FOR A GLOBAL TELECOMMUNICATION SOLUTIONS PROVIDER

FTI Cybersecurity was engaged, through external counsel, to investigate a corporate rival's fraudulent manipulation of their online reviews.

OUR IMPACT

We uncovered email communications, invoices, PayPal payments, expense reports, and subpoenaed technical data, including IPs, domain names, email addresses, and usernames, from review websites that tied the defendant to the fake review scheme. Relying on our findings, damages experts calculated damages north of $40 million, which persuaded the opposing side to settle.

OUR ROLE

Our team analyzed documents, obtained through discovery, and conducted significant open source intelligence gathering while developing a repeatable methodology to identify fake reviews with varying confidence levels as proof of the fraudulent scheme. We provided our findings in an expert report and deposition.

Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

Services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

MIKE DRISCOLL
Head of National Security
Senior Managing Director
+1 917 575 4435
mike.driscoll@fticonsulting.com

SARA MURRAY
National Security
Managing Director
+1 202 340 7167
sara.murray@fticonsulting.com

BRENT MCGOLDRICK
U.S. Digital, Strategic Communications
Senior Managing Director
+1 202 346 8861
brent.mcgoldrick@fticonsulting.com

ANTHONY J. FERRANTE
Global Head of Cybersecurity
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

JORDAN RAE KELLY
Head of Cybersecurity, Americas
Senior Managing Director
+1 202 312 9140
jordan.kelly@fticonsulting.com

FTI CONSULTING™